




Sistema Informativo Aziendale
Ufficio Comunicazione e Relazioni con il Pubblico

Norme interne
per il corretto uso
delle attrezzature e
dei servizi informatici



A cura di:
Francesco Moroncini
Luigi Sfredda
Concetta Trapè

Norme interne per il corretto uso delle attrezzature e dei servizi informatici

SOMMARIO

1.	PREMESSA GENERALE.....	4
2.	DEFINIZIONI	5
3.	IL RESPONSABILE DEL SIA.....	7
4.	DISPOSIZIONI GENERALI E AUTORIZZAZIONI	8
5.	MODALITÀ DI AUTORIZZAZIONE AI SERVIZI INFORMATICI	9
6.	UTILIZZO DEL PERSONAL COMPUTER	9
7.	UTILIZZO DI PC PORTATILI.....	10
8.	UTILIZZO DI STAMPANTI LOCALI E DI RETE	10
9.	GESTIONE DEGLI ACCESSI E DELLE PASSWORD	11
10.	UTILIZZO DELLA RETE LOCALE	11
11.	CARTELLA UTENTE PER IL SALVATAGGIO DEI DOCUMENTI E DATI DI LAVORO	12
12.	CARTELLE DI GRUPPO CONDIVISE	12
13.	UTILIZZO DEI SUPPORTI MAGNETICI.....	12
14.	CORRETTO UTILIZZO DELLA RETE INTERNET E DEI RELATIVI SERVIZI. CONTROLLI.	13
15.	USO DELLA POSTA ELETTRONICA.....	13
16.	PROTEZIONE ANTIVIRUS	14
17.	MODALITÀ E TEMPI DI CONSERVAZIONE DEI LOG (REGISTRAZIONI).....	15
18.	CONTROLLI E VERIFICHE (AUDIT INTERNI)	15
19.	OSSERVANZA DELLE DISPOSIZIONI IN MATERIA DI PRIVACY.....	15
20.	NON OSSERVANZA DELLA NORMATIVA AZIENDALE	15
21.	PRESCRIZIONI E SANZIONI	15

1. PREMESSA GENERALE

Le realtà aziendali si caratterizzano per l'elevato uso della tecnologia informatica che da un lato ha consentito l'introduzione di innovative tecniche di gestione dell'impresa, dall'altro ha dato origine a numerose problematiche relative all'utilizzo degli strumenti informatici forniti dalla Zona al dipendente per lo svolgimento delle proprie mansioni.

In questo senso, viene fortemente sentita dai datori di lavoro la necessità di porre in essere adeguati sistemi di controllo sull'utilizzo di tali strumenti da parte dei dipendenti e di sanzionare conseguentemente quegli usi scorretti che, oltre ad esporre la Zona stessa a rischi tanto patrimoniali quanto penali, possono di per sé considerarsi contrari ai doveri di diligenza e fedeltà previsti dagli artt. 2104 e 2105 del codice civile e dall'art. 23 del CCNL.

I controlli preventivi e continui sull'uso degli strumenti informatici devono garantire tanto il diritto del datore di lavoro di proteggere la propria organizzazione, essendo i computer aziendali strumenti di lavoro la cui utilizzazione personale è preclusa, quanto il diritto del lavoratore a non vedere invasa la propria sfera personale, e quindi il diritto alla riservatezza ed alla dignità come sanciti dallo Statuto dei lavoratori e dalla legge 196/2003 sulla tutela dei dati personali.

Le norme di seguito riportate vengono incontro a tali esigenze disciplinando le condizioni per il corretto utilizzo degli strumenti informatici da parte dei dipendenti, in particolare alla luce degli obblighi previsti dal Decreto Legislativo 30 giugno 2003 n. 196, relativo all'adozione delle misure minime di sicurezza per il trattamento dei dati personali.

La progressiva diffusione delle nuove tecnologie informatiche ed in particolare il libero accesso alla rete Internet dai Personal Computer, espone l'Amministrazione ai rischi di un coinvolgimento sia patrimoniale che penale, evidenti problemi per la sicurezza e l'immagine della Zona stessa.

L'utilizzo delle risorse informatiche e telematiche della Zona deve sempre ispirarsi al principio della diligenza e correttezza.

Le presenti norme interne sono dirette ad evitare che anche comportamenti inconsapevoli possano innescare problemi o minacce alla sicurezza nel trattamento dei dati.

Tali prescrizioni si aggiungono ed integrano le specifiche istruzioni che vanno fornite a tutti gli incaricati in attuazione del Decreto Legislativo 30 giugno 2003 n. 196 "Codice in materia di protezione dei dati personali".

2. DEFINIZIONI

Al fine delle presenti norme vengono riportate le seguenti definizioni, così come riportate nell'art. 4 del Decreto Legislativo 30 giugno 2003 n. 196:

- 2.1 **trattamento:** qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati;
- 2.2 **dato personale:** qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;
- 2.3 **dati identificativi:** i dati personali che permettono l'identificazione diretta dell'interessato;
- 2.4 **dati sensibili:** i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;
- 2.5 **dati giudiziari:** i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del D.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale;
- 2.6 **titolare:** la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza;
- 2.7 **responsabile:** la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali;
- 2.8 **incaricati:** le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;
- 2.9 **interessato:** la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali;
- 2.10 **comunicazione:** il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- 2.11 **diffusione:** il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- 2.12 **dato anonimo:** il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;

- 2.13 **blocco:** la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento;
- 2.14 **banca di dati:** qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti;
- 2.15 **Garante:** l'autorità di cui all'articolo 153, istituita dalla legge 31 dicembre 1996, n. 675.
- 2.16 **comunicazione elettronica:** ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico. Sono escluse le informazioni trasmesse al pubblico tramite una rete di comunicazione elettronica, come parte di un servizio di radiodiffusione, salvo che le stesse informazioni siano collegate ad un abbonato o utente ricevente, identificato o identificabile;
- 2.17 **chiamata:** la connessione istituita da un servizio telefonico accessibile al pubblico, che consente la comunicazione bidirezionale in tempo reale;
- 2.18 **reti di comunicazione elettronica:** i sistemi di trasmissione, le apparecchiature di commutazione o di instradamento e altre risorse che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, incluse le reti satellitari, le reti terrestri mobili e fisse a commutazione di circuito e a commutazione di pacchetto, compresa Internet, le reti utilizzate per la diffusione circolare dei programmi sonori e televisivi, i sistemi per il trasporto della corrente elettrica, nella misura in cui sono utilizzati per trasmettere i segnali, le reti televisive via cavo, indipendentemente dal tipo di informazione trasportato;
- 2.19 **rete pubblica di comunicazioni:** una rete di comunicazioni elettroniche utilizzata interamente o prevalentemente per fornire servizi di comunicazione elettronica accessibili al pubblico;
- 2.20 **servizio di comunicazione elettronica:** i servizi consistenti esclusivamente o prevalentemente nella trasmissione di segnali su reti di comunicazioni elettroniche, compresi i servizi di telecomunicazioni e i servizi di trasmissione nelle reti utilizzate per la diffusione circolare radiotelevisiva, nei limiti previsti dall'articolo 2, lettera c), della direttiva 2002/21/CE del Parlamento europeo e del Consiglio, del 7 marzo 2002;
- 2.21 **abbonato:** qualunque persona fisica, persona giuridica, ente o associazione parte di un contratto con un fornitore di servizi di comunicazione elettronica accessibili al pubblico per la fornitura di tali servizi, o comunque destinatario di tali servizi tramite schede prepagate;
- 2.22 **utente:** qualsiasi persona fisica che utilizza un servizio di comunicazione elettronica accessibile al pubblico, per motivi privati o commerciali, senza esservi necessariamente abbonata;
- 2.23 **dati relativi al traffico:** qualsiasi dato sottoposto a trattamento ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o della relativa fatturazione;
- 2.24 **dati relativi all'ubicazione:** ogni dato trattato in una rete di comunicazione elettronica che indica la posizione geografica dell'apparecchiatura terminale dell'utente di un servizio di comunicazione elettronica accessibile al pubblico;
- 2.25 **servizio a valore aggiunto:** il servizio che richiede il trattamento dei dati relativi al traffico o dei dati relativi all'ubicazione diversi dai dati relativi al traffico, oltre a quanto è necessario per la trasmissione di una comunicazione o della relativa fatturazione;

- 2.26 **posta elettronica:** messaggi contenenti testi, voci, suoni o immagini trasmessi attraverso una rete pubblica di comunicazione, che possono essere archiviati in rete o nell'apparecchiatura terminale ricevente, fino a che il ricevente non ne ha preso conoscenza.
- 2.27 **misure minime:** il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'articolo 31;
- 2.28 **strumenti elettronici:** gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento;
- 2.29 **sistema informativo:** l'insieme di dispositivi, programmi ed infrastruttura di rete;
- 2.30 **autenticazione informatica:** l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità;
- 2.31 **credenziali di autenticazione:** i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica;
- 2.32 **parola chiave:** componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica;
- 2.33 **profilo di autorizzazione:** l'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti;
- 2.34 **sistema di autorizzazione:** l'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente.
- 2.35 **scopi storici:** le finalità di studio, indagine, ricerca e documentazione di figure, fatti e circostanze del passato;
- 2.36 **scopi statistici:** le finalità di indagine statistica o di produzione di risultati statistici, anche a mezzo di sistemi informativi statistici;
- 2.37 **scopi scientifici:** le finalità di studio e di indagine sistematica finalizzata allo sviluppo delle conoscenze scientifiche in uno specifico settore.

3. IL RESPONSABILE DEL SIA

3.1 Il Responsabile del SIA è l'amministratore e responsabile del Sistema Informativo.

3.2 Il Responsabile del SIA:

- svolge le attività di amministrazione secondo le disposizioni previste dalla normativa vigente sulla tutela dei dati personali e sulle misure di sicurezza relative;
- ha il compito di generare, sostituire ed invalidare, in relazione agli strumenti e alle applicazioni informatiche utilizzate e secondo aggiornati criteri tecnici di sicurezza, le parole chiave ed i codici identificativi personali da assegnare agli incaricati del trattamento dei dati personali;
- adotta programmi antivirus, firewall ed altri strumenti sia software che hardware, che garantiscano, anche in relazione alle conoscenze acquisite in base al progresso tecnico, la sicurezza nel trattamento dei dati personali secondo i criteri generali stabiliti da Decreto Legislativo 30 giugno 2003 n. 196;

- ha il compito di controllare periodicamente l'efficienza dei sistemi, per verificarne la validità tecnica, anche secondo consolidati criteri di valutazione;
- deve altresì vigilare, secondo le prassi istituite ed in accordo con il titolare e con i responsabili, che gli incaricati al trattamento dei dati si attengano alle procedure di volta in volta indicate specificamente per iscritto anche in relazione all'applicazione delle misure organizzative, fisiche e logiche, sulla sicurezza nel trattamento secondo il dettato dalla normativa vigente;
- è responsabile del codice identificativo personale assegnatogli come Amministratore del Sistema e vigila ai fini di evitare e prevenire intrusioni, facendo adottare idonei programmi e verificando l'efficienza dei sistemi di protezione ed accesso con sistemi automatici di controllo.

3.3 Il Responsabile del SIA, per l'espletamento delle funzioni e mansioni assegnate, ha la facoltà in qualunque momento di accedere ai dati trattati da ciascun utente, ivi compresi gli archivi di posta elettronica, anche delegando a terzi con specifico mandato, in relazione agli scopi di volta in volta identificati.

4. DISPOSIZIONI GENERALI E AUTORIZZAZIONI

- 4.1 Il personal computer (fisso e mobile), le periferiche ed i relativi programmi e/o applicazioni – comprensivi di supporti e manuali - affidati al dipendente sono esclusivamente degli strumenti di lavoro.
- 4.2 Tutti gli strumenti assegnati vanno custoditi in modo appropriato, con la cura e attenzione del buon padre di famiglia.
- 4.3 Tali strumenti possono essere utilizzati solo per fini professionali (in relazione, ovviamente, alle mansioni assegnate) e non anche per scopi personali, tanto meno per scopi illeciti.
- 4.4 Il furto, il danneggiamento o lo smarrimento di tali strumenti devono essere prontamente segnalati al Responsabile del SIA.
- 4.5 Le apparecchiature informatiche assegnate non possono essere scollegate o spostate senza l'autorizzazione del Responsabile del SIA.
- 4.6 Non modificare la configurazione delle apparecchiature informatiche assegnate.
- 4.7 Non installare alcuna applicazione informatica o programma non autorizzati dal Responsabile del SIA;
- 4.8 Non utilizzare alcuna apparecchiatura non autorizzata dal Responsabile del SIA, nemmeno se trattasi di dispositivi personali.
- 4.9 Non permettere l'utilizzo delle apparecchiature informatiche a terzi non autorizzati dal Responsabile del SIA.
- 4.10 E' severamente vietato l'utilizzo di supporti contenenti dati (floppy, cd-rom, dvd-rom, pen-drive, nastri, etc.) sul proprio personal computer, senza l'autorizzazione preventiva del Responsabile del SIA.
- 4.11 Per tutte le operazioni che specificamente la prevedono ai sensi del presente Regolamento, l'autorizzazione preventiva del Responsabile del SIA può essere richiesta solamente dai Responsabili delle Unità Operative Zonali; a seguito della richiesta, un tecnico dei Sistemi Informativi provvederà ad eseguire l'operazione.

5. MODALITÀ DI AUTORIZZAZIONE AI SERVIZI INFORMATICI

- 5.1 L'accesso ai Servizi Informatici è consentito solo se regolarmente autorizzato dal Responsabile della singola Unità Operativa; l'autorizzazione è nominativa.
- 5.2 Il Responsabile consegna l'autorizzazione al Responsabile del SIA che provvede all'attivazione del profilo di autorizzazione sul sistema di controllo ed autenticazione;
- 5.3 L'Autorizzazione può essere sia a tempo indeterminato che a tempo determinato; in caso di autorizzazione a tempo indeterminato non sarà necessario ripresentare periodicamente la richiesta di autorizzazione. L'autorizzazione a tempo determinato viene concessa per particolari esigenze: ricerche, progetti e può essere anche legata alla scadenza del contratto di lavoro.
- 5.4 L'Autorizzazione potrà essere presentata su apposita modulistica a cura del Responsabile della singola Unità Operativa.
- 5.5 Tale regolamentazione è applicabile anche per l'utilizzo dei servizi Internet; nella modulistica di autorizzazione ai Servizi Informatici dovrà essere specificamente riportato se l'utente è autorizzato anche all'uso dei servizi Internet.
- 5.6 Il Responsabile del SIA si riserva di autorizzare a singoli o a gruppi di utenti, l'accesso a tipologie di siti Internet altrimenti non consentito, in base alle mansioni ed eventuali disposizioni concordate con i propri Responsabili.

6. UTILIZZO DEL PERSONAL COMPUTER

- 6.1 I Responsabili delle Unità Operative hanno il compito di verificare il corretto utilizzo delle risorse assegnate evitandone l'uso improprio o l'accesso da parte di personale non autorizzato, compreso l'utilizzo da parte di terzi di punti rete in luoghi non presidiati.
- 6.2 Il Personal Computer (o PC) affidato al dipendente è uno strumento di lavoro. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.
- 6.3 L'accesso all'elaboratore è protetto da password, che deve essere custodita dall'incaricato con la massima diligenza e non divulgata a nessuno e per nessun motivo. Le password devono essere utilizzate per l'accesso alla rete, per l'accesso a qualsiasi applicazione che lo preveda, per il salva schermo (screen saver) e per il collegamento ad Internet.
- 6.4 Non è consentito l'uso di programmi diversi da quelli distribuiti ufficialmente dal Sistema Informativo Zonale (D.Lgs. n. 518/1992 sulla tutela giuridica del software e Legge n. 248/2000 nuove norme di tutela del diritto d'autore).
- 6.5 Non è consentito installare autonomamente nessun tipo di programma proveniente dall'esterno senza la preventiva autorizzazione del Responsabile del SIA ed una richiesta da parte del Responsabile dell'Unità Operativa a cui è assegnato il PC.
- 6.6 Non è consentita l'attivazione della password di accensione (Bios), senza preventiva autorizzazione da parte del Responsabile del SIA.
- 6.7 Non è consentito a nessun utente di modificare le caratteristiche impostate sui PC assegnati, i punti rete di accesso e le configurazioni delle reti LAN/WAN presenti nelle sedi, salvo autorizzazione del Responsabile del SIA.

- 6.8 Il Personal Computer deve essere spento prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio: lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso. In ogni caso deve essere attivato lo screen saver e la relativa password.
- 6.9 Non è consentita l'installazione sul proprio PC o il collegamento alla rete LAN di dispositivi di memorizzazione o di comunicazione (ad esempio masterizzatori, modem, pc portatili, web cam ed apparati in genere), se non autorizzati preventivamente dal Responsabile del SIA.
- 6.10 Agli utenti incaricati del trattamento dei dati è fatto divieto l'accesso contemporaneo con lo stesso account da più macchine.
- 6.11 E' fatto altresì obbligo distruggere materialmente le copie di sicurezza o i supporti di tipo removibile (floppy, CD-Rom, nastri) non più utilizzati prima di gettarle nella spazzatura, come previsto dall'Allegato B, paragrafo 22, del Decreto Legislativo 30 giugno 2003 n. 196.
- 6.12 Non è consentita la conservazione nella macchina assegnata o in dispositivi e supporti di memorizzazione, di file a contenuto oltraggioso e/o discriminatorio per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e politica.

7. UTILIZZO DI PC PORTATILI

- 7.1 L'utente è responsabile del PC portatile assegnatogli dal Responsabile del SIA e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.
- 7.2 Ai PC portatili si applicano le regole di utilizzo previste per i PC connessi in rete.
- 7.3 In caso di utilizzo condiviso dei PC portatili è fatto obbligo cancellare tutti i documenti creati in ragione della propria attività, prima della riconsegna della macchina.
- 7.4 I PC portatili utilizzati all'esterno della propria sede (corsi, convegni, etc.), non devono essere lasciati incustoditi.
- 7.5 Eventuali configurazioni di tipo Accesso Remoto, dirette verso la rete aziendale o attraverso internet, devono essere autorizzate preventivamente dal Responsabile del SIA. E' vietato utilizzare le suddette connessioni all'interno delle strutture della Zona ancor più se contemporaneamente connessi alla rete LAN.
- 7.6 Il furto o lo smarrimento dei PC portatili deve essere prontamente segnalato al Responsabile del SIA.
- 7.7 E' vietato memorizzare nei PC portatili documenti riservati o contenenti informazioni che possano inficiare la sicurezza del Sistema Informativo Zonale; essi andranno memorizzati in cartelle criptate o adeguatamente protette

8. UTILIZZO DI STAMPANTI LOCALI E DI RETE

- 8.1 La stampa di documenti contenenti dati personali o riservati deve essere eseguita preferibilmente sulla stampante locale collegata. Qualsiasi modalità di stampa di tali documenti su stampanti di rete o remote può essere eseguita a condizione che vengano usate tutte le cautele e le particolari attenzioni volte ad evitare l'indebita lettura del loro contenuto da parte di terzi non autorizzati.

- 8.2 E' fatto obbligo distruggere manualmente o con apposito dispositivo tutti gli stampati prima di gettarli nella spazzatura.
- 8.3 E' buona regola evitare di stampare documenti di dimensioni eccessive su stampanti di rete o condivise, al fine di non occupare le risorse di rete.

9. GESTIONE DEGLI ACCESSI E DELLE PASSWORD

- 9.1 I profili utente, le autorizzazioni relative, gli account utente e le password di accesso sono gestite dal Responsabile del SIA.
- 9.2 Le password di ingresso alla rete, di accesso ai programmi e dello screen saver, sono previste ed attribuite dall'Responsabile del SIA al momento del primo accesso. È fatto obbligo all'utente di modificarle al primo utilizzo.
- 9.3 Le password devono essere lunghe almeno 8 caratteri, formate da lettere (maiuscole e/o minuscole), numeri e caratteri speciali quali & % ^ # \$, ricordando che lettere maiuscole e minuscole hanno significati diversi per i sistemi, evitando ovviamente contenuti di senso logico immediato che sono facilmente individuabili (per es. nomi/date di nascita e simili).
- 9.4 Le password utilizzate dagli incaricati al trattamento hanno una durata massima di tre mesi, trascorsi i quali devono essere sostituite.
- 9.5 La password deve essere immediatamente sostituita, dandone comunicazione al Responsabile del SIA, nel caso si sospetti che la stessa abbia perso la segretezza.
- 9.6 Qualora l'utente venisse a conoscenza delle password di altro utente, è tenuto a darne immediata notizia al Responsabile del SIA.
- 9.7 E' compito dei Responsabili comunicare tempestivamente eventuali cambi di mansione del personale che comportino modifiche o revoche di autorizzazione all'accesso alle risorse informatiche. Tale comunicazione verrà effettuata all'Unità Operativa Gestione Risorse Umane e al Responsabile del SIA.

10. UTILIZZO DELLA RETE LOCALE

- 10.1 Le unità di rete sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. E' vietato memorizzare su queste unità qualsiasi file non legato all'attività lavorativa.
- 10.2 Il Responsabile del SIA effettua regolare attività di controllo, di amministrazione e di backup delle unità di rete. Egli può in qualunque momento procedere alla rimozione sui PC degli incaricati e sulle unità di rete di ogni file o applicazione che riterrà essere pericolosi per la sicurezza del Sistema Informativo.
- 10.3 Al fine di garantire la corretta gestione delle politiche di sicurezza delle informazioni è fatto divieto replicare su dischi locali dei PC dati aziendali, banche dati e documenti sensibili senza esplicita autorizzazione del Responsabile del SIA, che provvederà all'adozione di adeguate misure quali la criptazione dei dati e il backup.
- 10.4 Le password d'ingresso alla rete e ai programmi sono segrete, non devono essere comunicate a nessuno e devono essere gestite secondo le procedure impartite. E' assolutamente proibito entrare nella rete o accedere a programmi con nomi utente diversi dai propri.

- 10.5 Non è consentito ai Responsabili collegare PC o altri dispositivi alla rete aziendale senza la preventiva autorizzazione scritta dell'Responsabile del SIA ed una verifica della conformità agli standard tecnici previsti.
- 10.6 E' buona regola la periodica (almeno semestrale) pulizia degli archivi, tramite cancellazione dei file obsoleti, inutili o duplicati.

11. CARTELLA UTENTE PER IL SALVATAGGIO DEI DOCUMENTI E DATI DI LAVORO

- 11.1 Ogni utente ha disponibile sul server uno spazio (cartella utente) da utilizzare per il salvataggio dei documenti e dei dati di lavoro. E' severamente vietato il salvataggio di dati personali dell'utente, con particolare riferimento a quelli sensibili.

12. CARTELLE DI GRUPPO CONDIVISE

- 12.1 Le condivisioni per ovvie ragioni di riservatezza e protezione (backup) devono risiedere solamente sui server, con i permessi per i soli autorizzati. Le eventuali condivisioni locali saranno progressivamente migrate sui sistemi centrali o in alternativa dovranno essere adottate tutte le misure di sicurezza necessaria in accordo con il Responsabile del SIA.
- 12.2 La struttura delle cartelle condivise è la seguente:
- Cartella UFFICIO (una per ciascuna Unità Operativa): in questa area ogni utente potrà accedere in lettura/scrittura (RW) per condividere file soltanto con gli altri utenti dello stesso gruppo/Ufficio;
 - Cartella PUBBLICA: in questa area ogni utente potrà accedere in lettura/scrittura (RW) per condividere file soltanto con gli altri utenti della stessa area omogenea, che saranno definite volta per volta secondo le necessità;
 - Cartella SCAMBIO: in questa area ogni utente potrà accedere in lettura/scrittura (RW) per scambiare file di grandi dimensioni con altri utenti della rete; tutto il contenuto dell'area Scambio sarà cancellato giornalmente.
- 12.3 Anche per queste aree di condivisione è severamente vietato il salvataggio di dati personali dell'utente con particolare riferimento a quelli sensibili.

13. UTILIZZO DEI SUPPORTI MAGNETICI

- 13.1 Tutti i supporti magnetici riutilizzabili (dischetti, cassette, cartucce, cd-r, dvd±r) contenenti dati sensibili devono essere trattati con particolare cautela al fine di evitare che il loro contenuto possa essere recuperato (All. B, paragrafo 22, del Decreto Legislativo 30 giugno 2003 n. 196). E' possibile infatti recuperare i dati memorizzati anche dopo la loro cancellazione.
- 13.2 I supporti magnetici contenenti dati sensibili devono essere custoditi in armadi chiusi a chiave.
- 13.3 Non è consentito caricare file contenuti in supporti magnetici/ ottici non aventi alcuna attinenza con la propria prestazione lavorativa.
- 13.4 Tutti i file di provenienza incerta, anche se potenzialmente attinenti all'attività lavorativa non devono essere utilizzati, installati, testati senza la preventiva autorizzazione

del Responsabile del SIA.

14. CORRETTO UTILIZZO DELLA RETE INTERNET E DEI RELATIVI SERVIZI. CONTROLLI.

- 14.1 Il PC abilitato alla navigazione in Internet costituisce uno strumento aziendale necessario allo svolgimento della propria attività lavorativa. Non è consentita la navigazione in Internet per motivi diversi da quelli funzionali all'attività lavorativa stessa.
- 14.2 E' fatto divieto all'utente lo scarico (download) di software gratuito (freeware) e shareware prelevato da siti Internet, se non preventivamente autorizzato dal Responsabile del SIA.
- 14.3 E' tassativamente vietata l'effettuazione di ogni genere di transazione finanziaria (operazioni di remote banking e acquisti on-line), salvo i casi direttamente autorizzati dal Responsabile dell'Unità Operativa.
- 14.4 E' da evitare ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa.
- 14.5 E' vietata la partecipazione a Forum non professionali, l'utilizzo di chat line, di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames), se non debitamente autorizzati dal Responsabile dell'Unità Operativa.
- 14.6 E' severamente vietato memorizzare sul disco locale del personal computer o sulla condivisione di rete documenti o file scaricati dal web contenenti dati personali.
- 14.7 Al fine di sovrintendere la sicurezza di tutto il sistema e di ottimizzare l'uso delle risorse, gli investimenti e le prestazioni delle connessioni esistenti, tutte le attività di navigazione degli utenti sono registrate automaticamente dai dispositivi di connessione alla rete Internet. Il Responsabile del SIA effettuerà dei controlli periodici e casuali sulla navigazione dei dipendenti. I controlli riguarderanno:
 - a) indirizzi e contenuti della navigazione
 - b) tempi di connessione
 - c) quantità di dati scaricati
- 14.8 Il Responsabile del SIA provvede alla conservazione delle registrazioni sulla navigazione effettuata dagli utenti per il periodo di un anno, a meno di diversa disposizione dell'Autorità Giudiziaria, dopodiché si provvederà alla loro cancellazione.
- 14.9 Il Responsabile del SIA periodicamente consegna ai Responsabili un report riepilogativo del traffico effettuato dai dipendenti della relativa Unità Operativa.
- 14.10 Il dipendente può richiedere, ai sensi dell'Art. 7 del D.Lgs. n. 196/03, il report del traffico personalmente effettuato.

15. USO DELLA POSTA ELETTRONICA

- 15.1 La casella di posta, assegnata all'utente, è uno strumento di lavoro. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.
- 15.2 Si rammenta che i sistemi di posta elettronica non consentono di garantire la riservatezza delle informazioni trasmesse (l'e-mail deve essere considerata come una cartolina postale): si raccomanda pertanto agli utenti di non inoltrare dati ed informa-

zioni classificabili "sensibili" o "riservate" con questo mezzo.

E' fatto divieto di utilizzare le caselle di posta elettronica aziendali per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail-list non attinenti la propria attività o funzione svolta per la Zona, salvo diversa ed esplicita autorizzazione del Responsabile dell'Unità Operativa.

- 15.3 E' buona norma cancellare senza aprirli, i 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. E' previsto un dimensionamento massimo per ciascuna casella in relazione alla disponibilità di spazio dei sistemi di posta di volta in volta disponibili, che non potrà essere superato per evitare l'appesantimento della gestione dei server stessi.
- 15.4 Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti, contenga impegni contrattuali o documenti da considerarsi riservati (in quanto contraddistinti dalla dicitura "strettamente riservati" o da dicitura analoga), deve essere visionata dal Responsabile dell'Unità Operativa cui si riferisce l'attività. E' opportuno fare riferimento alle procedure in essere per la corrispondenza ordinaria (gestione protocollo).
- 15.5 La trasmissione di file nell'ambito della Zona tramite la posta elettronica è possibile a condizione che la loro dimensione non superi 1 Mbyte. Per file di dimensioni maggiori si consiglia di utilizzare la cartella di scambio presente sui server, notificando a mezzo mail al destinatario la disponibilità del file stesso.
- 15.6 E' vietato attivare o lanciare (doppio click) gli allegati di messaggi anche se provenienti da persona conosciuta, a meno che non si tratti di documenti (zip, doc, xls, ecc.) al fine di evitare la propagazione di virus worm.
- 15.7 E' vietato effettuare modifiche alla configurazione o cancellare file seguendo istruzioni contenute in messaggi anche se provenienti da persona conosciuta (virus hoax).
- 15.8 E' vietato inviare messaggi di posta riconducibili alle cosiddette catene telematiche (o di Sant'Antonio). Nel caso si ricevano messaggi di questo tipo, dare comunicazione al Responsabile del SIA che potrà attivare appositi filtri.
- 15.9 E' vietato l'utilizzo di indirizzi di posta elettronica non preventivamente autorizzati dal Responsabile del SIA, con specifico riferimento alle web mail (Libero, Virgilio, Yahoo..)

16. PROTEZIONE ANTIVIRUS

- 16.1 Ogni utente deve tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico aziendale mediante virus o mediante ogni altro software aggressivo.
- 16.2 Ogni utente è tenuto a controllare il regolare funzionamento e l'aggiornamento periodico del software installato, secondo le procedure previste.
- 16.3 Nel caso che il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente:
 - a) sospendere ogni elaborazione in corso senza spegnere il computer;
 - b) segnalare l'accaduto al Responsabile del SIA.
- 16.4 Non è consentito l'utilizzo di floppy disk, cd rom, cd riscrivibili, nastri magnetici di provenienza ignota.

16.5 Ogni dispositivo magnetico di provenienza esterna alla Zona dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus, dovrà essere consegnato al Responsabile del SIA.

17. MODALITÀ E TEMPI DI CONSERVAZIONE DEI LOG (REGISTRAZIONI)

17.1 Tutte le attività dei sistemi informatici sono registrate in appositi archivi elettronici (log), adeguatamente conservati e protetti nei sistemi stessi o su supporti di memorizzazione. Solo il Responsabile del SIA o personale specificamente delegato può accedere a fini di controllo e di protezione.

17.2 A meno di diversa disposizione di legge o di provvedimento da parte dell'Autorità Giudiziaria, il tempo di conservazione delle registrazioni è di .

17.3 Il dipendente può richiedere, ai sensi dell'Art. 7 del D.Lgs. n. 196/03, tutte le registrazioni che lo riguardano.

18. CONTROLLI E VERIFICHE (AUDIT INTERNI)

18.1 L'Responsabile del SIA o personale specificamente delegato per iscritto, effettuerà dei controlli periodici o anche casuali su tutte le attività svolte utilizzando i sistemi.

18.2 I controlli riguarderanno ai sensi dell'art. 34 del D.Lgs. 196/03:

1. la sussistenza delle condizioni per la conservazione dei profili di autorizzazione (garanzia di riservatezza);
2. l'integrità delle informazioni contro alterazioni o danneggiamenti, tutelando l'accuratezza e la completezza dei dati (garanzia di integrità)
3. la disponibilità delle informazioni quando occorre e nell'ambito del contesto pertinente (garanzia di disponibilità)

18.3 Il Responsabile del SIA comunica alla Direzione di Zona qualsiasi comportamento non conforme al presente Regolamento per gli opportuni provvedimenti del caso;

19. OSSERVANZA DELLE DISPOSIZIONI IN MATERIA DI PRIVACY

19.1 E' obbligatorio attenersi alle disposizioni in materia di Privacy e di misure minime di sicurezza. Tale norma risulta indicata nelle lettere di individuazione dell'incaricato al trattamento dei dati ai sensi del Decreto Legislativo 30 giugno 2003 n. 196.

20. NON OSSERVANZA DELLA NORMATIVA AZIENDALE

20.1 Il mancato rispetto o la violazione delle norme del presente Regolamento è perseguibile con provvedimenti disciplinari nonché con le azioni civili e penali consentite.

21. PRESCRIZIONI E SANZIONI

21.1 In caso di utilizzo del Sistema Informativo non conforme alle norme del presente Regolamento o alle Leggi dello Stato, tenendo conto del principio di proporzionalità, fermo restando gli obblighi di legge, il Responsabile del SIA, a seguito di apposita procedura istruttoria:

- 21.1.1 disabilita il profilo utente, previa autorizzazione del Responsabile dell'Unità Operativa cui l'utente appartiene;
- 21.1.2 comunicare l'illecito al Responsabile dell'Unità Operativa cui l'utente appartiene, ai fini dell'applicazione degli eventuali provvedimenti disciplinari ai sensi delle Disposizioni in materia di disciplina del Personale della Zona (Delibera n. 430/DG del 23/10/2001);
- 21.2 Tale procedura potrà essere promossa anche su richiesta del Responsabile della singola Unità Operativa, che ha il dovere di coadiuvare in ogni caso l'attività del Responsabile del SIA.

Ancona, li _____

La Direzione

La R. S. U.